【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】令和6年8月28日(2024.8.28)

【国際公開番号】WO2023/112382
【出願番号】特願2023-567533(P2023-567533)
【国際特許分類】
G06F 21/55(2013.01)
G06F 21/62(2013.01)
【FI】
G06F 21/55 320
G06F 21/62

【手続補正書】
【提出日】令和6年4月22日(2024.4.22)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
監視対象において発生したイベントに関するローデータに基づいて行われる前記イベントにおける攻撃シナリオの分析を支援する分析支援装置において行われる分析支援方法であって、
前記監視対象と通信するか、または前記監視対象から取得した前記ローデータを記録するデータベースと通信することにより、前記ローデータを取得し、
取得した前記ローデータと類似しかつ過去に取得された前記ローデータに対する過去の分析結果を出力する、
分析支援方法。
【請求項２】
監視対象において発生したイベントに関するローデータに基づいて行われる前記イベントにおける攻撃シナリオの分析を支援する分析支援装置において行われる分析支援方法であって、
前記ローデータ、および前記ローデータに基づいてセキュリティ情報イベント管理装置によって判定された判定結果を取得し、
取得した前記ローデータおよび前記判定結果と類似しかつ過去に取得された前記ローデータおよび前記判定結果に対する過去の分析結果を出力する、
分析支援方法。
【請求項３】
取得した前記ローデータと過去に取得された１つ以上の前記ローデータのそれぞれとを照合し、
過去に取得された前記１つ以上のローデータのうち取得した前記ローデータと類似する前記ローデータがあるか否かを判定し、
当該ローデータがある場合、当該ローデータに対する前記分析結果を出力する、
請求項１または２に記載の分析支援方法。
【請求項４】
前記ローデータは、複数の項目を含み、
取得した前記ローデータに含まれる前記複数の項目の内容と過去に取得された前記１つ以上のローデータのそれぞれに含まれる前記複数の項目の内容とを照合し、

過去に取得された前記１つ以上のローデータのうち取得した前記ローデータに含まれる前記複数の項目の内容と同一の内容の前記複数の項目を含む前記ローデータがある場合、過去に取得された前記１つ以上のローデータのうち取得した前記ローデータと類似する前記ローデータがあると判定する、
請求項３に記載の分析支援方法。
【請求項５】
前記ローデータは、複数の項目を含み、
取得した前記ローデータに含まれる前記複数の項目の内容と過去に取得された前記１つ以上のローデータのそれぞれに含まれる前記複数の項目の内容とを照合し、
取得した前記ローデータに含まれる前記複数の項目のそれぞれの内容と過去に取得された前記１つ以上のローデータのそれぞれに含まれる前記複数の項目のうち当該項目と同一の項目の内容とが同一である場合には加点し、取得した前記ローデータに含まれる前記複数の項目のそれぞれの内容と過去に取得された前記１つ以上のローデータのそれぞれに含まれる前記複数の項目のうち当該項目と同一の項目の内容とが同一でない場合には加点しないまたは減点することによって、過去に取得された前記１つ以上のローデータのそれぞれのスコアを算出し、
過去に取得された前記１つ以上のローデータのうち算出されたスコアが所定の閾値以上の前記ローデータがある場合、過去に取得された前記１つ以上のローデータのうち取得した前記ローデータと類似する前記ローデータがあると判定する、
請求項３に記載の分析支援方法。
【請求項６】
前記ローデータは、複数の項目を含み、
過去に取得された１つ以上の前記ローデータは、前記複数の項目の内容毎に１つ以上のグループに分けられており、
前記１つ以上のグループのうち取得した前記ローデータに含まれる前記複数の項目の内容と同一の内容に係るグループがある場合には取得した前記ローデータを当該グループに属させ、前記１つ以上のグループのうち取得した前記ローデータに含まれる前記複数の項目の内容と同一の内容に係るグループがない場合には取得した前記ローデータを新たなグループに属させる、
請求項１または２に記載の分析支援方法。
【請求項７】
取得した前記ローデータに含まれる前記複数の項目の内容と前記１つ以上のグループのそれぞれに係る前記複数の項目の内容とを照合し、
前記１つ以上のグループのうち取得した前記ローデータに含まれる前記複数の項目の内容と同一の内容に係るグループがある場合、過去に取得された前記１つ以上のローデータのうち取得した前記ローデータと類似する前記ローデータがあると判定する、
請求項６に記載の分析支援方法。
【請求項８】
取得した前記ローデータに含まれる前記複数の項目の内容と前記１つ以上のグループのそれぞれに係る前記複数の項目の内容とを照合し、
取得した前記ローデータに含まれる前記複数の項目のそれぞれの内容と前記１つ以上のグループのそれぞれに係る前記複数の項目のうち当該項目と同一の項目の内容とが同一である場合には加点し、取得した前記ローデータに含まれる前記複数の項目のそれぞれの内容と前記１つ以上のグループのそれぞれに係る前記複数の項目のうち当該項目と同一の項目の内容とが同一でない場合には加点しないまたは減点することによって、前記１つ以上のグループのそれぞれのスコアを算出し、
前記１つ以上のグループのうち算出されたスコアが所定の閾値以上のグループがある場合、過去に取得された前記１つ以上のローデータのうち取得した前記ローデータと類似する前記ローデータがあると判定する、
請求項６に記載の分析支援方法。

【請求項９】
取得した前記ローデータと過去に取得された１つ以上の前記ローデータのそれぞれとを照合し、
過去に取得された前記１つ以上のローデータのうち取得した前記ローデータと類似する前記ローデータがあるか否かを判定し、
当該ローデータがある場合、当該ローデータに対する前記分析結果を閲覧する権限があるか否かを判定し、
前記権限がある場合、当該ローデータに対する前記分析結果を出力する、
請求項１または２に記載の分析支援方法。
【請求項１０】
監視対象において発生したイベントに関するローデータに基づいて行われる前記イベントにおける攻撃シナリオの分析を支援する分析支援装置であって、
前記監視対象と通信するか、または前記監視対象から取得した前記ローデータを記録するデータベースと通信することにより、前記ローデータを取得する取得部と、
取得した前記ローデータと類似しかつ過去に取得された前記ローデータに対する過去の分析結果を出力する出力部とを備える、
分析支援装置。
【請求項１１】
請求項１に記載の分析支援方法をコンピュータに実行させるためのプログラム。